Krestfield CRL OCSP Monitor

Installation and Configuration Guide

Version 2.0

Overview

The Krestfield CRL OCSP Monitor tracks and monitors the health of your revocation checking end points, alerting you to issues before there is any impact to your services

CRLs hosted on http and ldap end points can be monitored for validity, correctness, size and latency. OCSP servers can be queried to exercise the full request/response process and check for validity, correct status and response times

Real-time results can be viewed via the Management Console or via a generated web page. Test case failures are reported via logs (text based and windows event), email alerts can also be sent and scripts can be executed ensuring that the relevant support staff are notified as soon as an issue is identified

The Krestfield CRL OCSP Monitor is supported on the following operating systems:

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

The server requires the .NET Framework version 4.7.2 or above

Installation

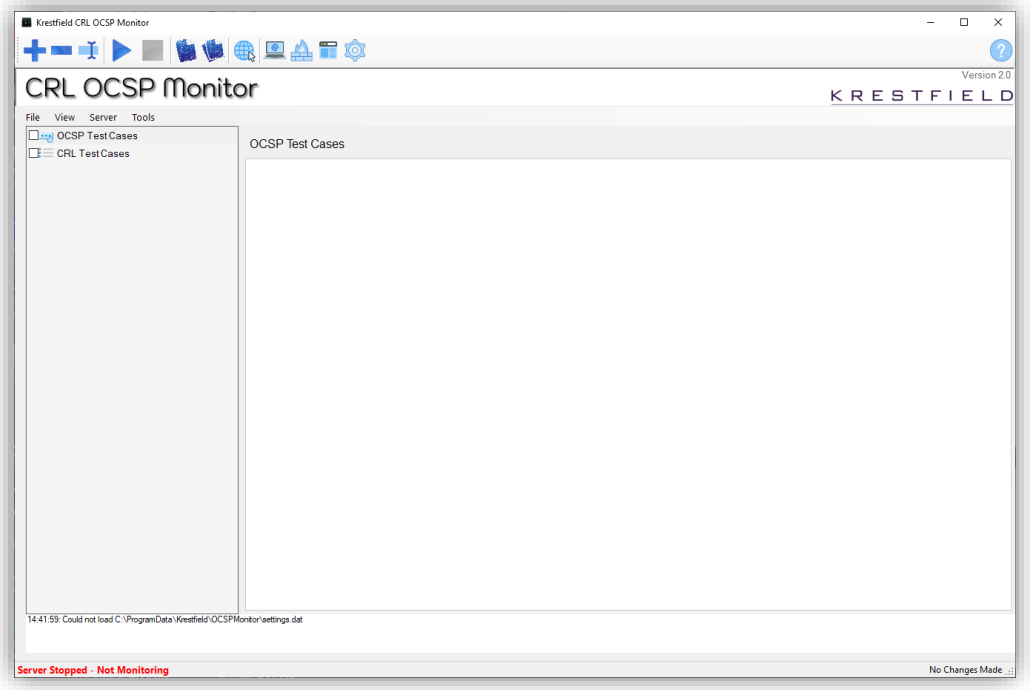
Double click the **SetupOCSPMonitorV2.0.msi** installation file and click **Next** throughout the screens, changing the Folder location if required

Configuration

Start the Management console by double clicking the desktop icon: 

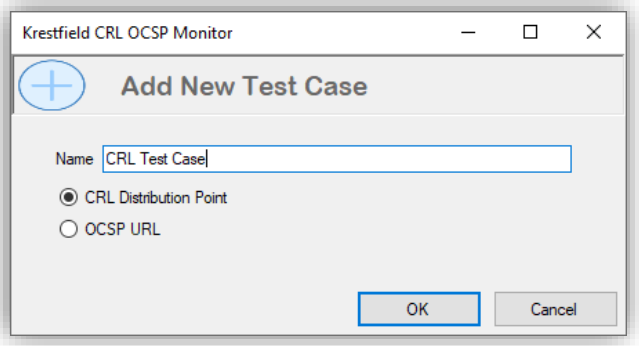
Or by starting the **Krestfield CRL OCSP Monitor Console** from the programs list

The following screen will be shown:

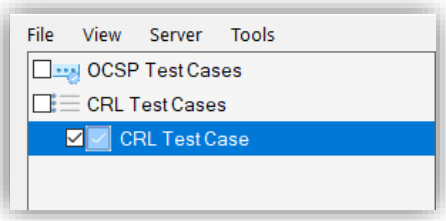


The first step will be to configure a test case

Click  to add a new Test Case



Enter a name for the test case and select whether this test case is to monitor a CRL end point or OCSP server. Click **OK**. Note: The name must be unique to ensure each test case is distinguishable from any others. The new test case will appear in the left hand pane:



The *settings* tab will now be available to populate. For CRL test cases this tab is called *CRL Settings* and for OCSP testcases, it is called *OCSP Settings*

On this settings tab enter either the **CRL URI** or **OCSP URL**

The CRL end point will be either a file, http URL or ldap address and must take the following form:

- http://
- ldap://
- file://

Note that for a local ldap address (such as in a Microsoft domain environment) the ldap address will start ldap:/// (i.e. three leading slashes) to indicate this is hosted on a local domain controller. Similarly, to reference a local file, the file location will start file:/// - again three leading slashes to indicate this is a local file

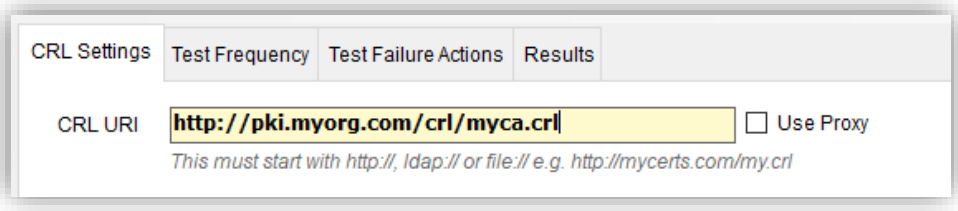
Examples of a valid CRL URI are:

```
http://pki.myorg.com/crl/myca.crl

file:///d:/crl/myorg.crl

file://\\crlserver\crl\ca1.crl

ldap:///CN=Org%20CA%201,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configur
ation,DC=MyOrg,Dc=com?certificateRevocationList?base?objectClass=cRLDistributionP
oint
```

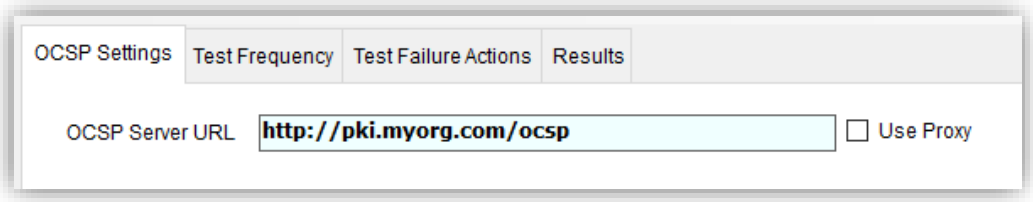


The OCSP URL will take the form:

- http(s)://

An examples of a valid OCSP URL is:

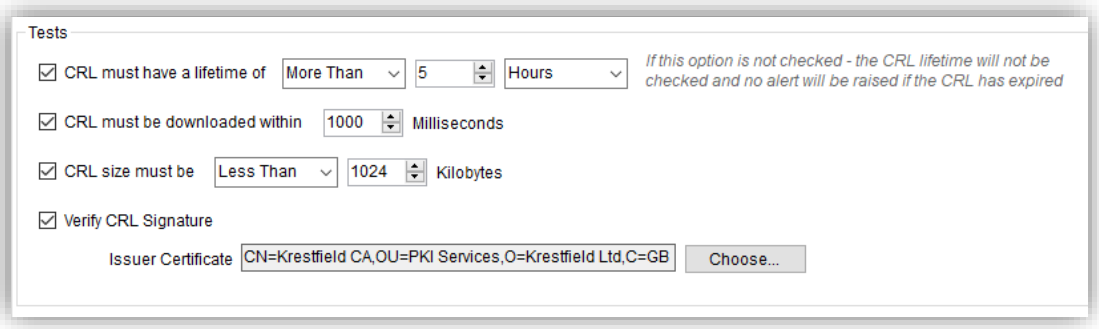
```
http://pki.myorg.com/ocsp
```



If the machine where the monitor is running can only access these end points via a proxy (for example, if you are monitoring external public facing end points from within a corporate network), click **Use Proxy** (you will need to enter the proxy server details later – see below)

CRL Test Case Settings

The following tests can be performed on a CRL



CRL must have a lifetime of

A CRL has an expiry data associated with it (defined by the *Next Update* field). A CRL whose Next Update time is after the current time has expired and clients will reject the CRL (and revocation checking will fail)

To test that the CRL lifetime is of a certain period, check the **CRL must have a lifetime of** check box and set the options of More Than/Less Than and the time period required

Test cases can be used to ensure that a CRL is being generated in good time (before they are due to expire) but also that CRLs are adhering to any policy (e.g. to verify that a maximum CRL lifetime is not being exceeded)

It is recommended to set this option to ensure that CRLs do not expire unexpectedly. Generally, a new CRL should be generated and published well before the previous CRL expires (such that their lifetimes overlap) in order provide ample time to deal with any fresh CRL generation issue

CRL must be downloaded within

If you wish to also check the CRL is downloaded within a certain time, check the **CRL must be downloaded within** check box and specify the number of milliseconds. If it takes longer than this period for the CRL to be downloaded the test case will fail

This test is useful to verify the availability of the CRL and responsiveness of the hosting server

CRL size must be

To be informed when a CRL exceeds a maximum size, or to ensure it is the minimum expected size, check the **CRL size must be** check box and set the More Than or Less Than option and size in Kilobytes. The test will fail if the CRL file size is not within these limits

Verify CRL Signature

CRLs are usually signed by the Certificate Authority that issued them. This signature can be verified by checking the **Verify CRL Signature** check box

This option also requires that the issuing certificate (i.e. the CA certificate) is specified. Click **Choose…** to navigate to the CA certificate

This test will confirm that the CRL was indeed signed by the correct issuer CA and will highlight if a CRL is incorrectly signed, the signature is somehow corrupt or an attempt has being made to sign the CRL with a different CA certificate

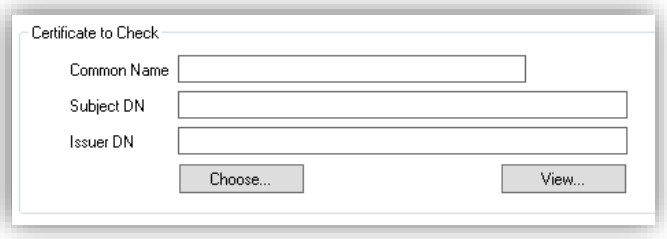
Certificate to Check

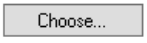
If a certificate is specified here, its status will then be checked against the CRL. This option can be used to confirm that a revoked certificate is included in the CRL (or that a known valid certificate is not)

To enable this check the **Check Specific Certificate Status** check box and click **Choose…** to navigate to the required certificate file

OCSP Test Case Settings

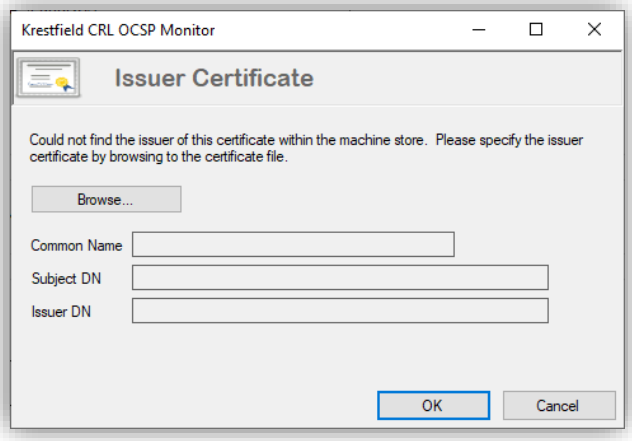
For an OCSP Test Case a certificate, whose status is to be checked against the server, must be specified. This can be any certificate that would have been issued from the CA associated with the OCSP server being monitored



Click 

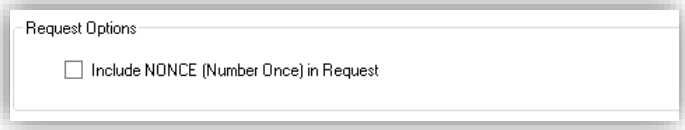
and navigate to the chosen certificate file. Click **OK**

If the issuer of the certificate is not recognised (this can happen if the issuer certificate is not configured in the local windows store) you will be prompted to specify the intermediate as well:



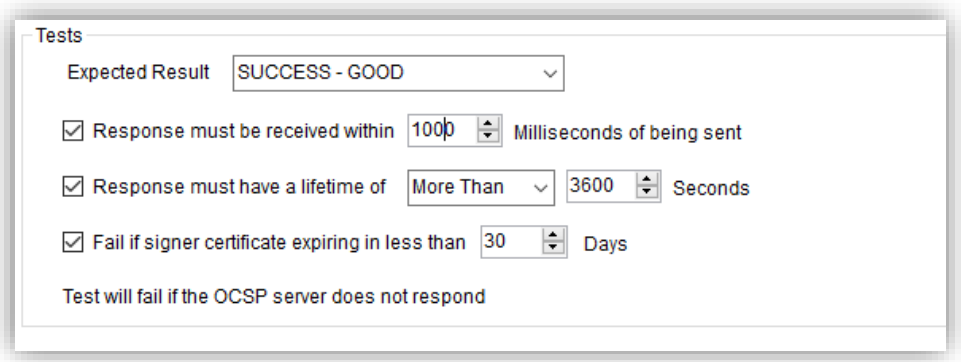
Navigate to the correct issuer certificate file and click **OK**

Next, choose if you wish a NONCE (Number Once) to be sent in the request



If this is configured, the CRL OCSP Monitor will send a random number in the request and verify that the same number is present in the response. This forces the OCSP Server to generate a fresh response (and not return a cached version)

Next select the tests that you want to be carried out



Expected Result

This is the response you expect to be received from the OCSP server when returning the status of the certificate specified in the previous step

You can choose from the following options:

- SUCCESS – GOOD: *The certificate is known and has not been revoked*
- SUCCESS – REVOKED: *The certificate is known but has been revoked*
- SUCCESS – UNKNOWN: *The certificate is not known*
- ERROR - TRY LATER: *The OCSP server is busy or some other issue is preventing it from responding at this time*
- ERROR - SIGNATURE REQUIRED: *There is a requirement for the request to have been signed and it has not been. Note: the current version does not support OCSP request signing however, this is planned for future releases*
- ERROR - UNAUTHORIZED: *The requestor is not authorised to obtain a response from this server. This can happen if the request is signed by an untrusted or unknown certificate*

The following can be configured but are unlikely to be returned in any environment other than development

- ERROR - INTERNAL ERROR: *The OCSP server has experienced an internal error*
- ERROR - MALFORMED REQUEST: *The OCSP request was not formatted correctly or is corrupt*

As long as the responder returns the response specified, the test case will pass

E.g. If in the previous step you specified a revoked certificate you would set the status to **SUCCESS – REVOKED** and as long as the OCSP returned this response, the test case will succeed

Responses must be received within

If you wish to also check the responses are returned within a certain time, check the **Response must be received within** check box and specify the number of milliseconds. If it takes longer than this period for the response to be returned the test case will fail

Response must have a lifetime of

To check that the OCSP response has a certain lifetime (that is the period from the current time to the next update time) then check the **Response must have a lifetime of** check box and specify the time. This may be used to confirm that responses are being produced with short lifetimes (e.g. five minutes), or are producing responses with the expected *next update* values

Fail if signer certificate expiring in less than

OCSP Responses are signed. If the certificate used to sign the response has expired, the response will be rejected by the client (and revocation checking will fail). In order to check the lifetime of the signing certificate, check the **Fail if signer certificate expiring in less than** check box and specify the number of days

For example, if you set this to 30 days and the signer certificate is expiring in 29 days, the test case will fail and an alert can be sent indicating that a renewal should take place

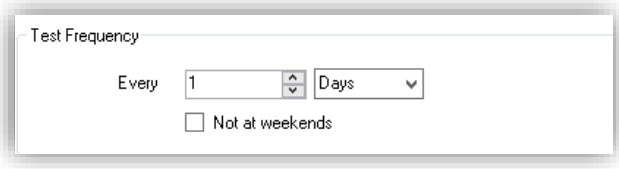
If the OCSP signing certificate is auto-renewed (as can be configured with the Microsoft OCSP Responder) set this time to the renewal period as configured on the certificate template, to ensure the auto-renewal is operating correctly

Note that if the responder does not return any response the test case will fail anyway

Test Frequency Tab

This is the frequency that the test case will run. The range is from 1 second to a number of days

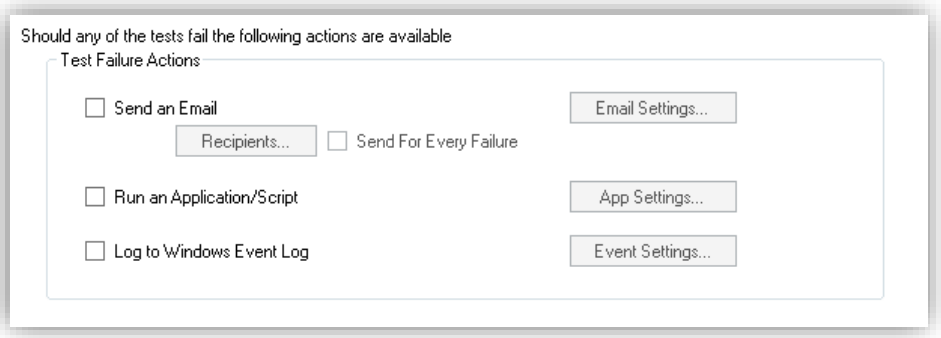
Usually a number of minutes (e.g. 5 minutes) is sufficient for monitoring OCSP servers. CRLs may not require as regular monitoring but these intervals are dependant on the purpose of the test case



If you do not wish the tests to run at weekends check the **Not at Weekends** button

Test Failure Actions Tab

This section defines what to do should a test case fail



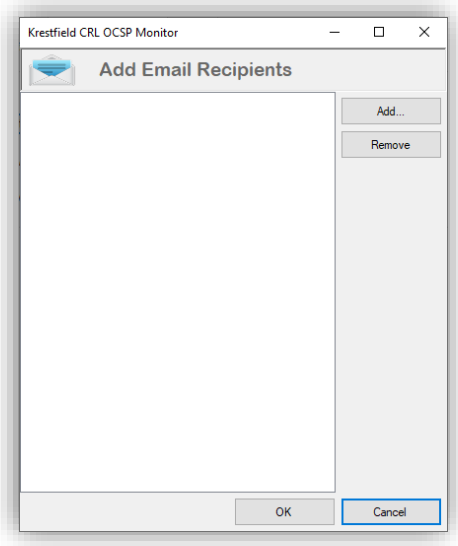
The options are

- Send an Email

  If you wish certain individuals/teams to be emailed should the test case fail, check the **Send an Email** checkbox

  The Email Settings must also be set for this to operate. See the section below on Email Server Settings for details on how to configure this

  You can then specify the recipients by clicking the **Recipients** button. The following dialog will appear:



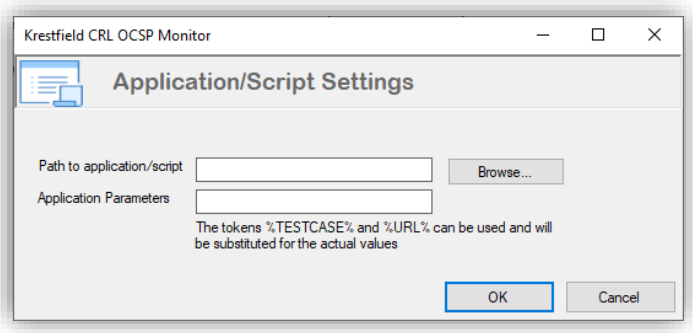
Use the **Add** and **Remove** buttons to add or remove email addresses to the available list of recipients. Note: the list of available email addresses is global, in that other test cases will also see the same list of email addresses

Click **OK** to save the email addresses

Normal behaviour is that an email will be sent when a test case initially fails and not for subsequent failures. However, if you wish an email to be sent at every test failure, check the **Send for Every Failure** check box

- Run an Application/Script

  To execute an application or script when a test case fails, check this option. Click the **App Settings...** button and browse to the application or script. Add any script parameters as required and click **OK**



For example, if you wish to run a powershell script you would set Path to application/script as:

```
powershell.exe
```

and for application parameters, set the script name and additional parameters. e.g.

```
c:\scripts\alert.ps1 %TESTCASE% %URL% %ERROR%
```

In this example, these parameters could be accessed in alert.ps1 as follows:

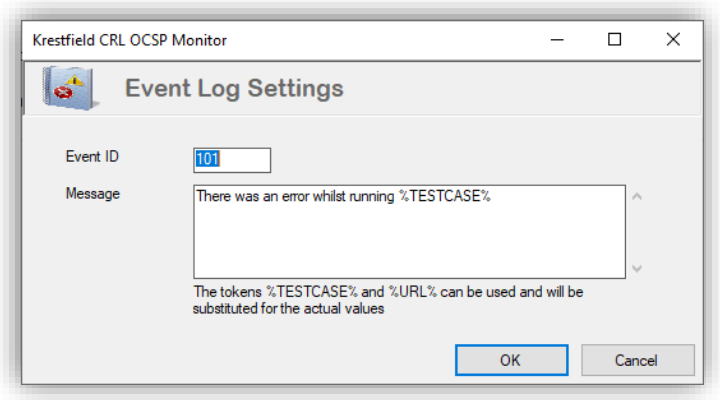
```
$testCaseName = $args[0]
$testCaseUrl = $args[1]
$testCaseError = $args[2]
```

This allows for advanced reporting and alerting capabilities such as raising tickets in ServiceNow

Note: The account running the CRL OCSP Monitor service must have permissions to execute the application/script chosen. If this is tied to specific users/groups you may wish to run the service under a specific account or an account in the same group. See Running the Service under a different account below

- Log to Windows Event Log

  To log an event to the Windows Event Log, check this option. This is useful for alerting systems that may already be able to monitor the Event Log
  Choose **Event Settings...** to set the Event ID and message that will appear in the log entry



Note that the failure reason will automatically be included in the event log entry

Once all settings have been configured click the **Apply** button to save

Starting/Stopping the Service

To start the service you can click the **Start Server** button from the Management Console, or manually start the service from the windows services window

To stop the service you can click the **Stop Server** button from the Management Console, or manually stop the service from the windows services window

The service will appear within the Windows Services list as: **Krestfield OCSP Monitor Service**

Note: There is no need to start and stop the service following any configuration updates made in the Management Console. The service will automatically detect changes to the configuration and start using the new settings

By default the service is configured to start automatically. This means that if the host machine is restarted the service will automatically start

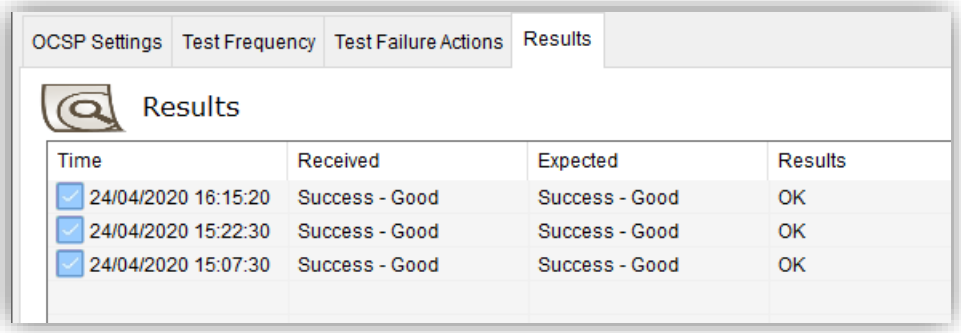
To change this to a manual process, open the Windows Services screen, right click the **Krestfield OCSP Monitor** service and change the Startup type to **manual**

Viewing Logs

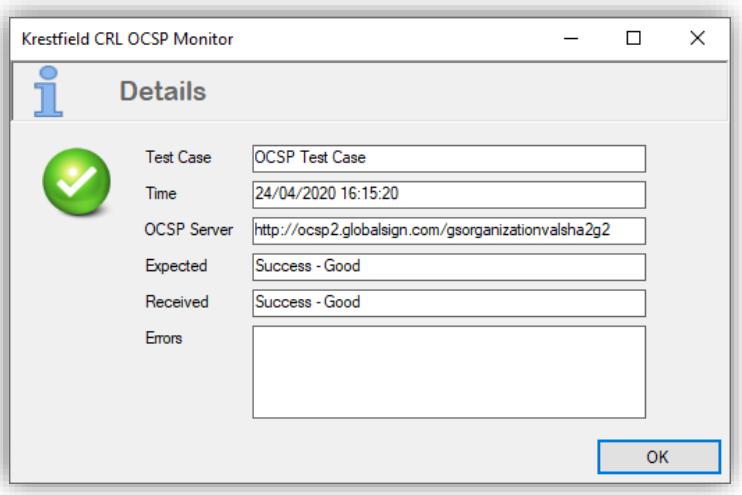
The CRL OCSP Monitor creates several logs:

Live Status Logs - Per Test Case

These logs can be viewed from the Management Console. To view, select a Test Case from the Test Case list and choose the **Results** tab as shown below:



The last day's results will be displayed. Each entry's details can be viewed by double clicking:

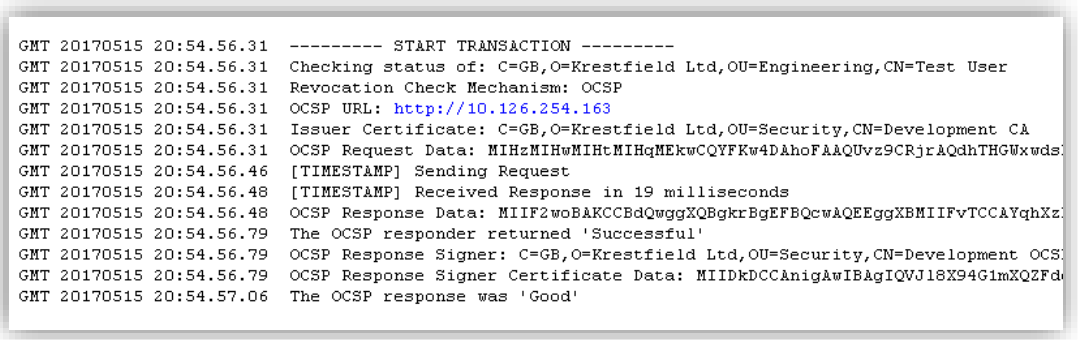


Detailed - Per Test Case

These logs show detailed information on every transaction including the downloading of CRLs and OCSP request and response data

To open, click on the 

button from the **Results** tab. The log file will be opened:



```
GMT 20170515 20:54.56.31  --------- START TRANSACTION ---------
GMT 20170515 20:54.56.31  Checking status of: C=GB,O=Krestfield Ltd,OU=Engineering,CN=Test User
GMT 20170515 20:54.56.31  Revocation Check Mechanism: OCSP
GMT 20170515 20:54.56.31  OCSP URL: http://10.126.254.163
GMT 20170515 20:54.56.31  Issuer Certificate: C=GB,O=Krestfield Ltd,OU=Security,CN=Development CA
GMT 20170515 20:54.56.31  OCSP Request Data: MIHzMIHwMIHtMIHqMEkwCQYFKw4DAhoFAAQUvz9CRjrAQdhTHGWxwds
GMT 20170515 20:54.56.46  [TIMESTAMP] Sending Request
GMT 20170515 20:54.56.48  [TIMESTAMP] Received Response in 19 milliseconds
GMT 20170515 20:54.56.48  OCSP Response Data: MIIF2woBAKCCBdQwggXQBgkrBgEFBQcwAQEEggXBMIIFvTCCAYqhXz
GMT 20170515 20:54.56.79  The OCSP responder returned 'Successful'
GMT 20170515 20:54.56.79  OCSP Response Signer: C=GB,O=Krestfield Ltd,OU=Security,CN=Development OCS
GMT 20170515 20:54.56.79  OCSP Response Signer Certificate Data: MIIDkDCCAnigAwIBAgIQVJl8X94G1mXQZFd
GMT 20170515 20:54.57.06  The OCSP response was 'Good'
```

Note: All test case log files can be opened at once by hitting the  button

Service Log

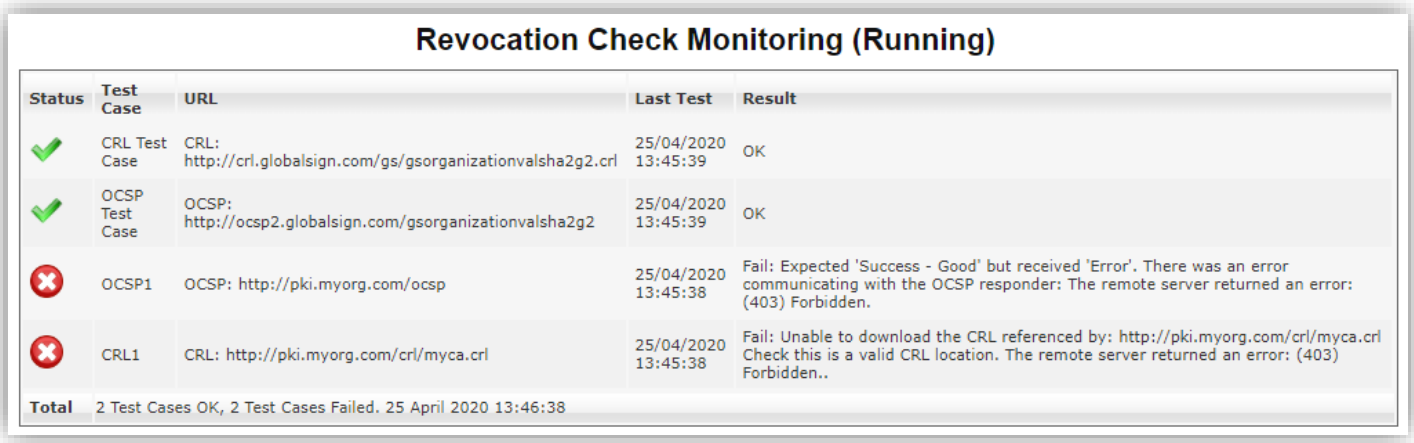
The service log displays information relating to the service such as start and stop events

It also displays high level test case success or failure information

To view the log click on the  button

Web Page Summary Settings

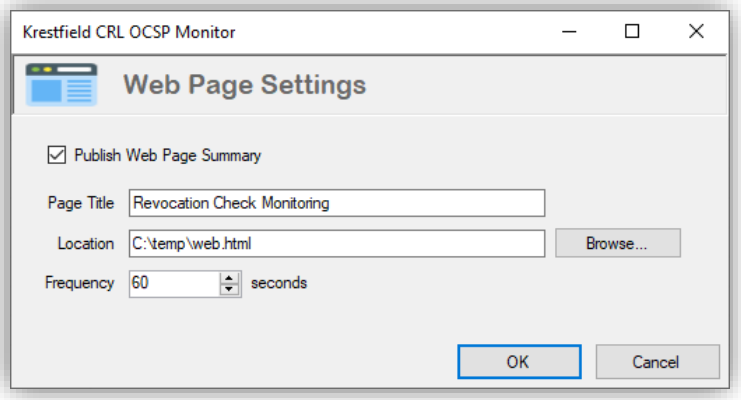
For high level monitoring an html status page can be configured to display status information which is continually updated. An example of this is shown below:



Revocation Check Monitoring (Running)

Status	Test Case	URL	Last Test	Result
✓	CRL Test Case	CRL: http://crl.globalsign.com/gs/gsorganizationvalsha2g2.crl	25/04/2020 13:45:39	OK
✓	OCSP Test Case	OCSP: http://ocsp2.globalsign.com/gsorganizationvalsha2g2	25/04/2020 13:45:39	OK
✗	OCSP1	OCSP: http://pki.myorg.com/ocsp	25/04/2020 13:45:38	Fail: Expected 'Success - Good' but received 'Error'. There was an error communicating with the OCSP responder: The remote server returned an error: (403) Forbidden.
✗	CRL1	CRL: http://pki.myorg.com/crl/myca.crl	25/04/2020 13:45:38	Fail: Unable to download the CRL referenced by: http://pki.myorg.com/crl/myca.crl Check this is a valid CRL location. The remote server returned an error: (403) Forbidden..
Total	2 Test Cases OK, 2 Test Cases Failed. 25 April 2020 13:46:38			

In order to configure this click the  button. The following dialog will be displayed:



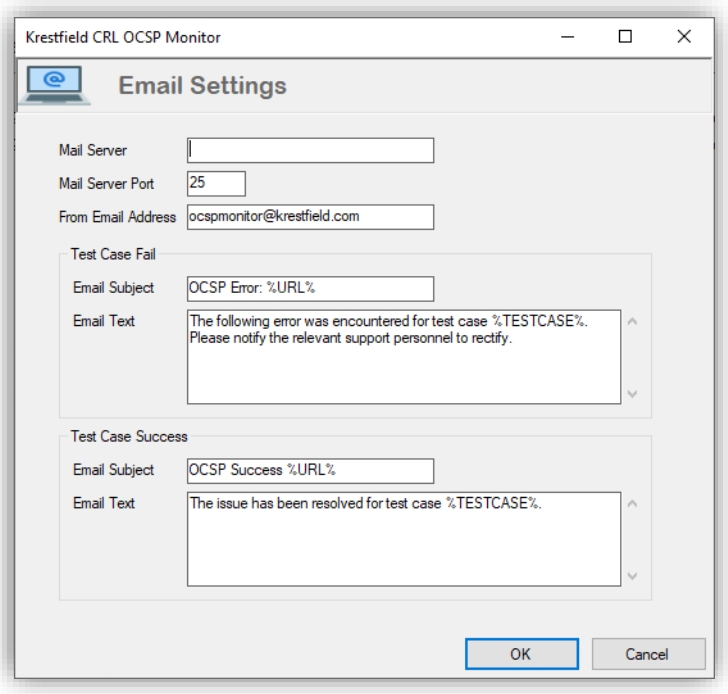
Check the **Publish Web Page Summary** check box

Set the page title, the html page location (this could be on a web server or local file system but should be accessible via the browser used to display the information), set the frequency (at which the page will be updated) and click **ok**

An html page with the name specified will now be produced and updated at the interval selected

Email Server Settings

In order to send emails the tool requires the smtp email server details. To configure these click the  button. The following dialog will be displayed



Enter the email server address, port and from address. The subject and text for failure and success emails can also be specified

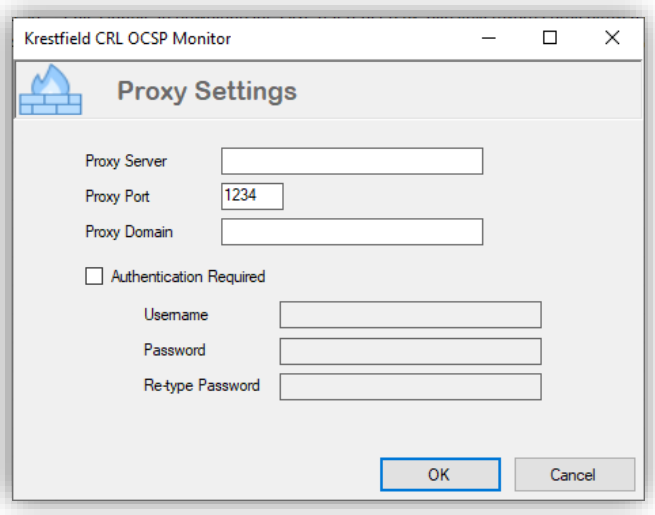
The %URL% and %TESTCASE% tags can be added anywhere in the subject or text. These tags will be substituted for the actual OCSP URL and test case name in the emails sent

In addition to the Email Text configured further information detailing the test case and exact error will also be included in the emails

Proxy Settings

If the monitor is being operated behind a proxy (e.g. as used in most corporate environments) the proxy server details can be set. Note that the test case OCSP URL or CRL URL must also have the *Use Proxy* option ticked to tunnel via the proxy server configured here

In order to set the proxy settings click the  button. The following dialog will be displayed:

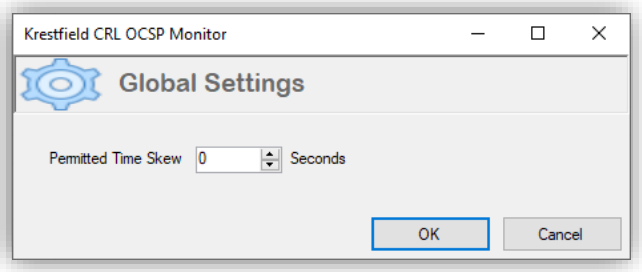


Enter details for the proxy server, port and domain. If authentication is required tick the Authentication Required box and enter the username and password

Click OK to save the settings

Global Settings

Open the Global Settings dialog by clicking on the button:



The only option available here is the **Permitted Time Skew**

This setting operates across all test cases and specifies the allowed amount of time drift between the monitors time and the OCSP servers time

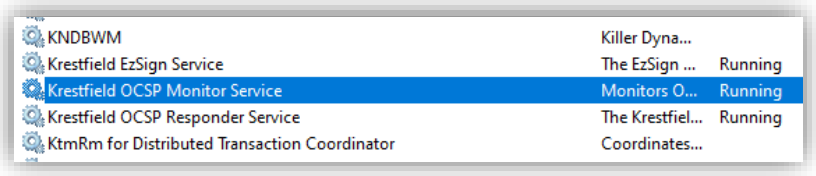
If the clocks between the OCSP Server and the machine hosting the CRL OCSP Monitor are not precisely synchronised errors may be experienced due to OCSP responses appearing to be produced before the current local time, or after the NextUpdate time

To prevent this set the **Permitted Time Skew** to an acceptable value (in seconds) which will cater for any time drift

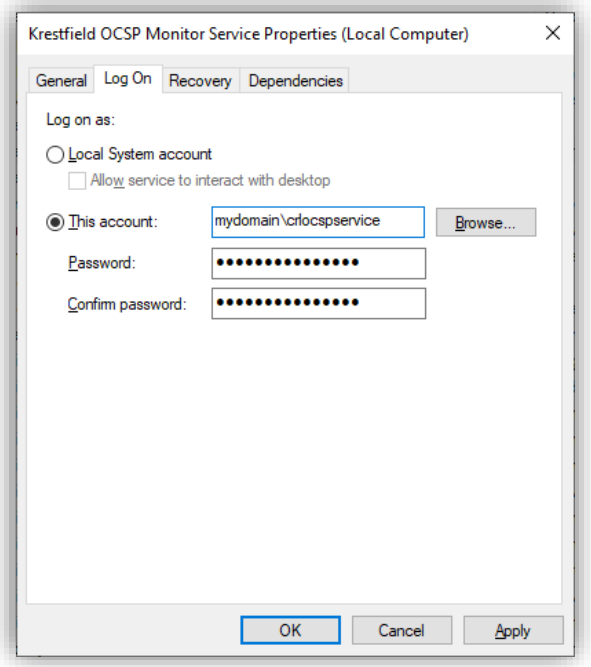
Running the Service under a different account

By default, when the service is installed it runs under the Local System account. This is normally sufficient for most cases but you may wish to run the service under a dedicated service account. This will allow, for example, the setting of permissions on any applications or scripts that may be called by the service. Where you would set execute permissions on these scripts/applications for the same account the service is running under (or group it is a members of)

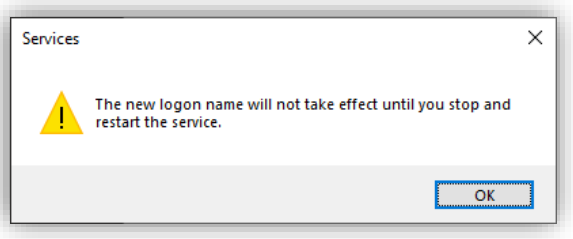
from windows, click **Start** and type **Services**. Select the **Services** app



Locate the **Krestfield OCSP Monitor Service**, right click and select **Properties**



Select the **Log On** tab, select This account and enter the account name and password. Click **OK**



Click **OK**

Now select the service again and click the **restart button**

Support

If you experience any issues with the Krestfield CRL OCSP Monitor or require help or advice on any aspects of the systems setup, contact support via email at **support@krestfield.com**

Please state the company name and if you have been issued one, your support agreement ID

Further details about this and other products are available from the Krestfield site:
https://www.krestfield.com